*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

DATE(S) ISSUED:
12/16/2009

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox and SeaMonkey Could Allow Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in the Mozilla Firefox and Mozilla SeaMonkey applications which could allow remote code execution. Mozilla Firefox is a popular web browser used to access the Internet. Mozilla SeaMonkey is a cross platform Internet suite of tools ranging from a web browser to an email client. The Mozilla applications (Firefox and SeaMonkey) utilize the same framework to display application specific information (e.g. Web pages, emails, chats).

Exploitation may occur if a user visits a webpage or opens a malicious file specifically crafted to take advantage of these vulnerabilities. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:

* Mozilla Firefox versions 3.0.15 and earlier
* Mozilla Firefox versions 3.5.5 and earlier
* Mozilla SeaMonkey versions 1.1.17 and earlier
* Mozilla SeaMonkey version 2.0

RISK:

Government:
* Large and medium government entities: High
* Small government entities: High

Businesses:
* Large and medium business entities: High
* Small business entities: High

Home users: High

DESCRIPTION:

Multiple vulnerabilities have been discovered in Mozilla Firefox and Mozilla SeaMonkey that could allow an attacker to take complete control of an affected system. Details of these vulnerabilities are:

Crashes with Evidence of Memory Corruption (mfsa2009-65)
Multiple remote memory corruption vulnerabilities affect Firefox and the JavaScript Engine. These issues can be exploited to cause the browser to crash and to possibly execute arbitrary code.

Memory Safety Bugs in Media Library (mfsa2009-660)
A remote code execution vulnerability affects the third-party 'liboggplay' library that is used in Firefox. This issue can be exploited to cause the browser to crash; arbitrary code execution may also be possible.

Integer Overflow in Theora Video Library (mfsa2009-67)
An integer-overflow vulnerability exists in the Theora video library ('libtheora') when large video dimensions are handled. An attacker can exploit this issue to execute arbitrary code in the context of the user running the affected browser.

NTLM Reflection Vulnerability (mfsa2009-68)
Mozilla Firefox and SeaMonkey are prone to an NTLM authentication reflection attack in which NTLM credentials from one application could be forwarded to another application via the web browser. Successful exploitation could allow an attacker to force NTLM authenticated requests on behalf of the user.

Local Bar Spoofing Vulnerabilities (mfsa2009-69)
Multiple issues allow attackers to carry out location bar spoofing attacks which may cause users to be unknowingly redirected to malicious websites.

Chrome Privilege Escalation (mfsa2009-70)
A privilege-escalation vulnerability affects the 'window.opener' property. An attacker can exploit this issue to execute malicious JavaScript with chrome privileges.

Information Disclosure Vulnerability (mfsa2009-71)
An information disclosure issue may allow attackers to enumerate installed COM objects using 'GeckoActiveXObject' exception messages.

RECOMMENDATIONS:
The following actions should be taken:

* Install the Mozilla patches and upgrades immediately after appropriate testing.
* Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
* Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.

REFERENCES:

Security Focus:
http://www.securityfocus.com/bid/37349

Secunia:
http://secunia.com/advisories/37699

Mozilla:
http://www.mozilla.org/security/announce/2009/mfsa2009-65.html
http://www.mozilla.org/security/announce/2009/mfsa2009-66.html
http://www.mozilla.org/security/announce/2009/mfsa2009-67.html
http://www.mozilla.org/security/announce/2009/mfsa2009-68.html
http://www.mozilla.org/security/announce/2009/mfsa2009-69.html
http://www.mozilla.org/security/announce/2009/mfsa2009-70.html
http://www.mozilla.org/security/announce/2009/mfsa2009-71.html

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3979
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3980
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3981
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3982
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3983
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3984
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3985
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3986
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3987
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3388
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-3389